

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION**

CALAB EVERLING , on behalf of himself and all others similarly situated, Plaintiff, v. FIRST MERCHANTS BANK , Defendant.	Case No. _____ JURY TRIAL DEMANDED
---	--

CLASS ACTION COMPLAINT

Plaintiff Calab Everling, individually and on behalf of all similarly situated persons, alleges the following against First Merchants Bank (“FMB” or “Defendant”) based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against FMB for its failure to properly secure and safeguard Plaintiff’s and other similarly situated FMB customers’ sensitive information, including full names, contact information, dates of birth, Social Security numbers, financial accounts information, and other sensitive information ("personally identifiable information" or “PII”).

2. Defendant is an Indiana based regional bank that offers personal banking, mortgage lending, and wealth management services to consumers in Indiana, Illinois, and Ohio ¹

¹ <https://www.firstmerchants.com/about> (last accessed July 19, 2023).

3. Upon information and belief, former and current Defendant customers are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain financial services from Defendant. Defendant retains this information for at least many years and even after the consumer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about June 21, 2023, Defendant learned that one its IT vendors had been penetrated by a cyberattack and that “certain FMB data may have been copied without authorization from their . . . system between May 28 and May 30, 2023.”² In response, Defendant “properly conducted a detailed review of the data involved to determine the types of information present and to whom it related.”³ As a result of its investigation, Defendant concluded—on an undisclosed date—that Plaintiff’s and Class Members’ PII was compromised in the Data Breach.⁴

6. According to Defendant’s Notice of Data Incident letter (the “Notice Letter”), the compromised PII included individuals’ names; contact information (including telephone numbers, addresses, and email addresses); dates of birth; Social Security numbers or tax identification numbers; mother’s maiden names; online/mobile banking usernames; company identification numbers; and/or financial account information, including account and routing numbers, as well as payee information.⁵

² The “Notice Letter”. A sample copy is available at <https://www.firstmerchants.com/moveit-data-incident> (last accessed July 19, 2023).

³ *Id.*

⁴ *Id.*

⁵ *Id.*

7. Defendant failed to adequately protect Plaintiff's and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) Plaintiff's PII being disseminated on the dark web; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

11. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. PARTIES

12. Plaintiff Calab Everling, is, and at all times mentioned herein was, an individual citizen of the Elwood, Indiana.

13. Defendant First Merchants Bank is an Indiana corporation with its principal place of business located at 200 East Jackson Street, Muncie, Indiana 47305.

III. JURISDICTION AND VENUE

14. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Indiana and have different citizenship from FMB. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

15. This Court has jurisdiction over FMB because FMB operates in this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and FMB has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Business*

17. Defendant is an Indiana based regional bank that offers personal banking, mortgage lending, and wealth management services to consumers in Indiana, Illinois, and Ohio.⁶

18. Plaintiff and Class Members are current and former FMB customers.

19. As a condition of receiving its products and/or services, FMB requires that its customers, including Plaintiff and Class Members, entrust it with highly sensitive personal information.

20. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

21. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining products and/or services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

⁶ <https://www.firstmerchants.com/about> (last accessed July 19, 2023).

22. Indeed, Defendant's Privacy Policy provides that: "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."⁷

23. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

25. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep consumer's PII safe and confidential.

26. Defendant had obligations created by FTC Act, Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

27. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

⁷ <https://www.firstmerchants.com/agreements-disclosures/privacy-policy> (last accessed July 19, 2023).

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

B. *The Data Breach*

29. On or about July 3, 2023, Defendant began sending Plaintiff and other Data Breach victims a Notice of Data Incident letter (the "Notice Letter"), informing them that:

What Happened? FMB uses vendors to manage technology and its customers' banking experience. One such vendor that provides services to many financial institutions used a third-party service, MOVEit Transfer ("MOVEit"), which has recently reported a security vulnerability. FMB understands that this incident has impacted a large number of companies across various industries, including government agencies, healthcare, and financial services. On June 21, 2023, the vendor confirmed to FMB that certain FMB data may have been copied without authorization from their MOVEit system between May 28 and May 30, 2023. FMB promptly conducted a detailed review of the data involved to determine the types of information present and to whom it related.

What Information Was Involved? Through its investigation of this incident, we have determined that the customer information potentially affected varies by individual or business, but may include: name; contact information, including telephone number, address, and email address; date of birth; Social Security number or tax identification number; mother's maiden name; online/mobile banking username; company identification number; and/or financial account information, including account and routing numbers, as well as payee information. Online or mobile banking passwords were not captured or compromised and remain unaffected by this incident.

What We Are Doing. We take the confidentiality, privacy, and security of information very seriously and we take the utmost care in selecting vendors to support our banking services. We are continuing to work with the vendor involved in this incident to investigate this issue and, as part of our ongoing commitment to information security, we are reviewing existing policies and procedures regarding vendor services and working to evaluate additional measures and safeguards in response to this incident.⁸

30. Omitted from the Notice Letter were the dates of Defendant's investigation, the date that Defendant first became aware of the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a

⁸ Notice Letter.

breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

31. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

33. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers and other sensitive information. Plaintiff’s and Class Members’ PII was accessed and stolen in the Data Breach.

34. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

C. Data Breaches Are Preventable

35. Defendant could have prevented this Data Breach by, among other things, properly encrypting PII being shared with its vendors or otherwise ensuring that such PII was protected while in transit or accessible.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

37. The unencrypted PII of Class Members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

38. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁹

39. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, customers and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

⁹ How to Protect Your Networks from RANSOMWARE, at 3, *available at*: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Oct. 17, 2022).

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁰

40. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates

¹⁰ *Id.* at 3-4.

- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].¹¹

41. Given that Defendant was storing and sharing the PII of its current and former customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

42. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach

¹¹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

and the exposure of the PII of thousands of current and former customers, including that of Plaintiff and Class Members.

D. *Defendant Acquires, Collects, And Stores Plaintiff's and the Class's PII*

43. As a condition to obtain products and/or services from FMB, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendant.

44. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its services.

45. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

47. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

48. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

49. Indeed, Defendant's Privacy Policy provides that: "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."¹²

50. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

E. *Defendant Knew or Should Have Known of the Risk Because Financial Institutions In Possession Of PII Are Particularly Susceptable To Cyber Attacks*

51. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting financial institutions that collect and store PII, like Defendant, preceding the date of the breach.

52. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

53. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹³

54. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.¹⁴

55. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report

¹² <https://www.firstmerchants.com/agreements-disclosures/privacy-policy> (last accessed July 19, 2023).

¹³ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

¹⁴ *Id.*

explained, smaller entities that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁵

56. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

57. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

¹⁵https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

60. Additionally, as companies became more dependent on computer systems to run their business,¹⁶ *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁷

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals’ detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. In the Notice Letter, Defendant makes an offer to cover identity monitoring services for a period of no longer than 24 months. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members’ PII. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

63. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members’ sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

64. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

¹⁶<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁷ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

65. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

66. As a financial institution in possession of its customers' and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

F. *Value Of Personally Identifiable Information*

67. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁸ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."¹⁹

68. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.²⁰

¹⁸ 17 C.F.R. § 248.201 (2013).

¹⁹ *Id.*

²⁰ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Oct. 17, 2022).

69. For example, PII can be sold at a price ranging from \$40 to \$200.²¹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²²

70. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—names and Social Security numbers.

71. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”²³

72. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

73. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁴

²¹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Oct. 17, 2022).

²² *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 21, 2022).

²³ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Oct. 17, 2022).

²⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 17, 2022).

G. *FMB Failed to Comply with FTC Guidelines*

74. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

75. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

76. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

77. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

78. These FTC enforcement actions include actions against financial institutions, like Defendant.

79. As evidenced by the Data Breach, FMB failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. FMB's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

80. FMB was at all times fully aware of its obligation to protect the PII of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

H. *FMB Failed to Comply with the Gramm-Leach-Bliley Act*

81. FMB is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

82. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

83. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant

time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.

84. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version becoming effective on October 28, 2014.

85. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

86. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be “clear and conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s] privacy policies and practices.” 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution’s security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided “so that each consumer can reasonably be expected to

receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

87. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers’ PII and storing that PII on Defendant's network systems.

88. Defendant failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers’ PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

89. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards’ key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

90. As alleged herein, Defendant violated the Safeguard Rule.

91. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

92. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

I. *FMB Failed to Comply with Industry Standards*

93. As noted above, experts studying cybersecurity routinely identify financial institutions as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

94. Some industry best practices that should be implemented by financial institutions dealing with sensitive PII, like FMB, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

95. Other best cybersecurity practices that are standard in the financial industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

96. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

97. Defendant failed to comply with these accepted standards in the financial industry, thereby permitting the Data Breach to occur.

J. *FMB Breached its Duty to Safeguard Plaintiff's and Class Members' PII*

98. In addition to its obligations under federal and state laws, FMB owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. FMB owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class Members

99. FMB breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. FMB's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

- b. Failing to adequately protect customers' PII;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
- e. Failing to sufficiently train its employees and vendors regarding the proper handling of its customers PII;
- f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- g. Failing to adhere to the Gramm-Leach-Bliley Act and industry standards for cybersecurity as discussed above; and
- h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

100. FMB negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

101. Had FMB remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

K. Common Injuries & Damages

102. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals,

the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; I invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Victims' Risk Of Identity Theft

103. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

104. The unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

105. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

106. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take

on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

107. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

108. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.²⁵

109. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

110. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

²⁵ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/) (last visited on May 26, 2023).

information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

111. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

112. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

113. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

114. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

115. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice Letter instructs, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

116. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result

of the Data Breach, such as changing passwords and contacting credit bureaus to secure their accounts.

117. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁶

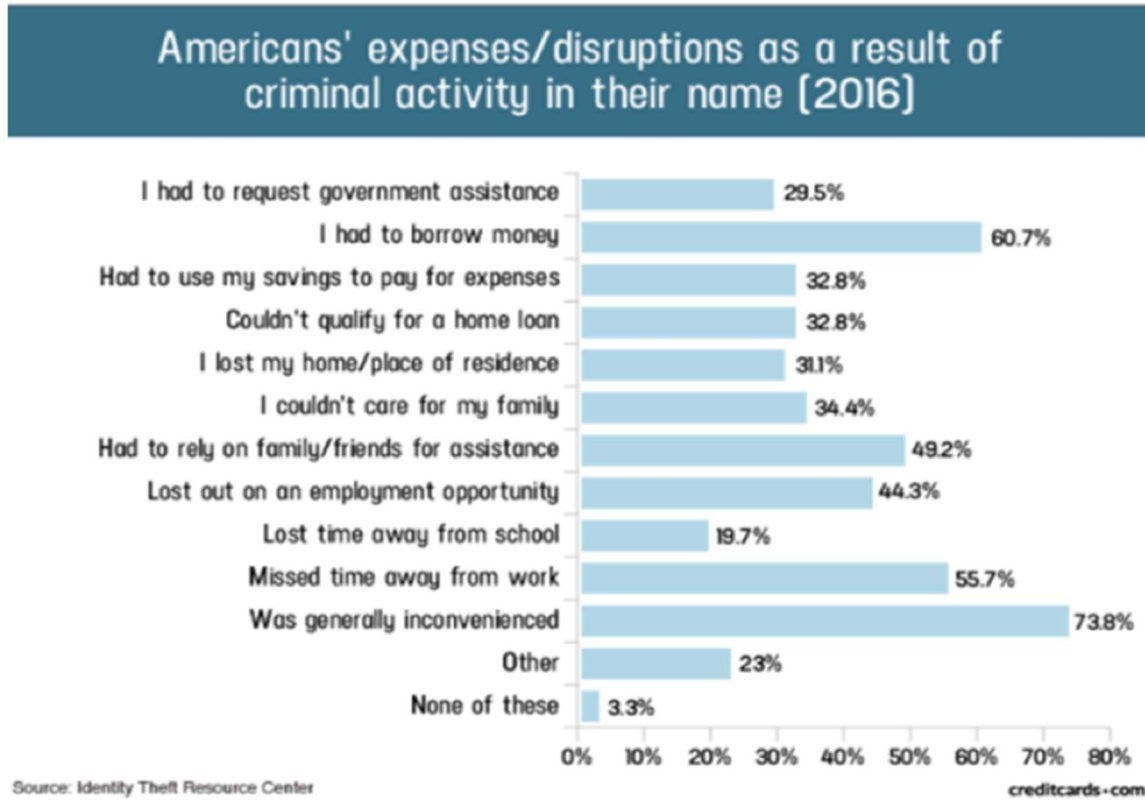
118. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁷

119. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:²⁸

²⁶ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

²⁷ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited July 7, 2022).

²⁸ Credit Card and ID Theft Statistics” by Jason Steele, 10/24/2017, at: <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Sep 13, 2022).



120. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁹

Diminution Value Of PII

121. PII is a valuable property right.³⁰ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison

²⁹ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Sep. 13, 2022) (“GAO Report”).

³⁰ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

122. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.³¹

123. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{32,33}

124. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁴

125. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.³⁵

126. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

127. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

³¹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

³² <https://datacoup.com/>

³³ <https://digi.me/what-is-digime/>

³⁴ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html>

³⁵ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Sep. 13, 2022).

breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change, e.g., names and Social Security numbers.

128. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

129. The fraudulent activity resulting from the Data Breach may not come to light for years.

130. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

131. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s network, amounting to thousands of individuals’ detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

132. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

133. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the

black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

134. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

135. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

136. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant’s Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant’s failure to safeguard their PII.

Loss Of The Benefit Of The Bargain

137. Furthermore, Defendant’s poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

L. *Plaintiff Everling's Experience*

138. Plaintiff Calab Everling is a former FMB customer who had a FMB account from approximately 2021 to 2022.

139. In order to open a FMB account, he was required to provide his PII to Defendant, including his name, Social Security number, date of birth, contact information, and financial account information.

140. At the time of the Data Breach—approximately May 28, 2023, through May 30, 2023—Defendant retained Plaintiff's PII in its system.

141. Plaintiff Everling is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

142. Plaintiff Calab Everling received the Notice Letter, by U.S. mail, directly from Defendant, dated July 3, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name; contact information, including telephone number, address, and email address; date of birth; Social Security number or tax identification number; mother's maiden name; online/mobile banking username; company identification number; and/or financial account information, including account and routing number, as well as payee information.

143. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including changing passwords and contacting credit bureaus to secure his accounts. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other

activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

144. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) an increase in spam calls, texts, and/or emails; (ii) his PII being disseminated on the dark web; (iii) lost or diminished value of his PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (v) invasion of privacy; (vi) loss of benefit of the bargain; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

145. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

146. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

147. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

148. Plaintiff Calab Everling has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

149. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

150. Specifically, Plaintiff proposes the following Nationwide Class, subject to amendment as appropriate:

Nationwide Class

All individuals in the United States whose PII was impacted as a result of the Data Breach (the "Class").

151. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

152. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

153. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

154. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

155. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether FMB engaged in the conduct alleged herein;
- b. Whether FMB's conduct violated the FTCA and/or GBLA;
- c. When FMB learned of the Data Breach;
- d. Whether FMB's response to the Data Breach was adequate;
- e. Whether FMB unlawfully lost or disclosed Plaintiff's and Class Members' PII;
- f. Whether FMB failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;
- g. Whether FMB's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether FMB's data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether FMB owed a duty to Class Members to safeguard their PII;
- j. Whether FMB breached its duty to Class Members to safeguard their PII;
- k. Whether hackers obtained Class Members' PII via the Data Breach;
- l. Whether FMB had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- m. Whether FMB breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

- n. Whether FMB knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiff and Class Members suffered as a result of FMB's misconduct;
- p. Whether FMB's conduct was negligent;
- q. Whether FMB was unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

156. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of FMB. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

157. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

158. Predominance. FMB has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from FMB's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

159. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for FMB. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

160. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). FMB has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

161. Finally, all members of the proposed Class are readily ascertainable. FMB has access to the names and addresses and/or email addresses of Class Members affected by the Data

Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by FMB.

VI. CLAIMS FOR RELIEF

COUNT I NEGLIGENCE (ON BEHALF OF PLAINTIFF AND THE CLASS)

162. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

163. Defendant requires its customers, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its financial services.

164. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its clients and its clients' customers, which solicitations and services affect commerce.

165. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

166. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

167. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

168. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

169. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

170. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

171. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between FMB and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted FMB with their confidential PII, a necessary part of being customers of Defendant.

172. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

173. Defendant was subject to an “independent duty,” untethered to any contract between Defendant and Plaintiff or the Class.

174. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

175. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

176. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

177. Defendant breached its duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
- d. Allowing unauthorized access to Class Members' PII;
- e. Failing to detect in a timely manner that Class Members' PII had been compromised;
- f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,

- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

178. Defendant violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

179. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

180. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes negligence.

181. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

182. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

183. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was

reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial industry.

184. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

185. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

186. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

187. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

188. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

189. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

190. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

191. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

192. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

193. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) Plaintiff's PII being disseminated on the dark web; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

194. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

195. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long

as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

196. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

197. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

198. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE CLASS)

199. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

200. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

201. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

202. As a skilled entity in the financial industry that possesses the sensitive PII of its current and former customers, Defendant owed a duty of care in protecting Plaintiff's and Class Members' PII, pursuant to Section 5 of the FTC Act, GLBA, and an independent duty of care.

203. Defendant violated Section 5 of the FTC Act, GLBA, and similar state statutes by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

204. In its Privacy Policy, FMB promises its customers that it will not disclose customers' PII, outside of the excepted circumstances set forth therein—none of which apply here. However, Plaintiff's and Class Members' PII has been disclosed without their written authorization as a result of the Data Breach.

205. Through its Privacy Policy, and in light of the highly sensitive and personal nature of the information FMB acquires and stores with respect to its customers, FMB promises to, among other things: keep customers' PII private; comply with industry standards related to data security and the maintenance of its customers' PII; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' PII; only use and release customers' PII for reasons that relate to the services it provides; and provide adequate notice to customers if their PII is disclosed without authorization.

206. As evidenced by the occurrence of the Data Breach, Defendant negligently misrepresented its data security measures and Privacy Policy to Plaintiff and Class Members.

207. As a skilled entity, Defendant violated Section 5 of the FTC Act and GLBA by negligently misrepresenting its data security practices to Plaintiff and Class Members.

208. As a skilled entity, Defendant violated Section 5 of the FTC Act and GLBA by breaching its duties of care to Plaintiff and Class Members, as provided in its Privacy Policy.

209. Defendant further violated Section 5 of the FTC Act and GLBA by failing to ensure that its vendors use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and shared and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

210. Defendant's violation of Section 5 of the FTC Act, GLBA, and other duties (listed above) constitutes negligence *per se*.

211. Class members are consumers within the class of persons Section 5 of the FTC Act, GLBA, and similar state statutes were intended to protect.

212. Moreover, the harm that has occurred is the type of harm the FTC Act, GLBA, and similar state statutes were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against financial institutions which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

213. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

214. There is a close causal connection between Defendant's failure to implement or ensure security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in

safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

215. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) Plaintiff's PII being disseminated on the dark web; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

216. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

217. As a direct and proximate result of Defendant's negligence *per se*, the products and/or services that Defendant provided to Plaintiff and Class Members damaged other property, including the value of their PII.

218. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

219. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

220. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

221. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

222. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

223. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving financial services from Defendant.

224. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

225. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

226. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

227. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

228. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

229. In accepting the PII of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

230. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

231. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

232. Plaintiff and Class Members paid money and provided their PII to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

233. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

234. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

235. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

236. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

237. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

238. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

239. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

240. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

241. This count is pleaded in the alternative to the Breach of Implied Contract claim above (Count III).

242. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or its agents and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their PII protected with adequate data security.

243. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

244. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

245. Defendant acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

246. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and

secure their PII, they would have entrusted their PII at Defendant or obtained services at Defendant.

247. Plaintiff and Class Members have no adequate remedy at law.

248. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

249. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) Plaintiff's PII being disseminated on the dark web; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

250. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

251. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate

based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

- xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;
- E. For an award of punitive damages, as allowable by law;
- F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;
- G. Pre- and post-judgment interest on any amounts awarded; and
- H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: July 25, 2023

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Phone: (866) 252-0878

gklinger@milberg.com

Counsel for Plaintiff and the Proposed Class